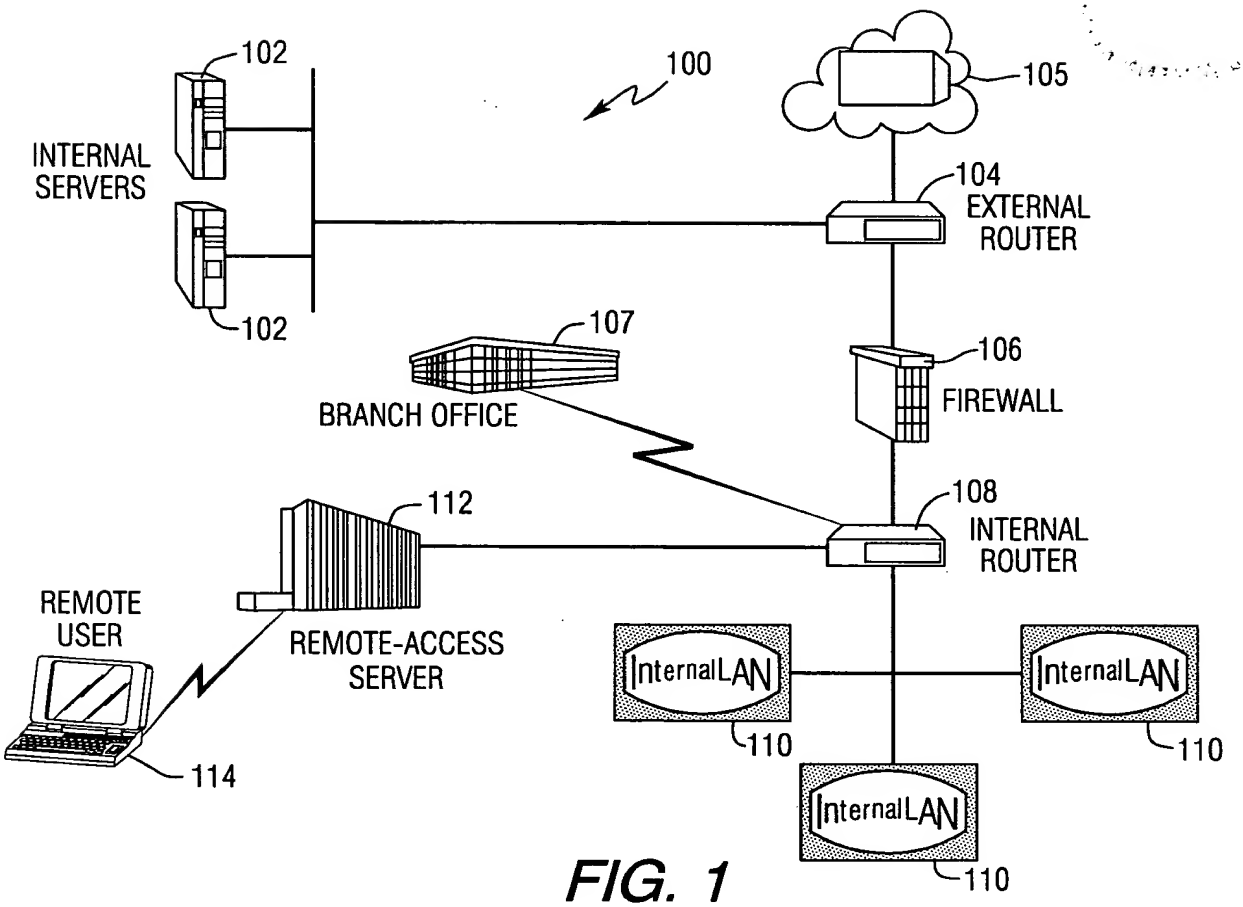

102
100
105
INTERNAL SERVERS
104
EXTERNAL ROUTER
102
107
106
BRANCH OFFICE
FIREWALL
112
108
INTERNAL ROUTER
REMOTE USER
REMOTE-ACCESS SERVER
InternalLAN
InternalLAN
110
110
InternalLAN
110
114

FIG. 1

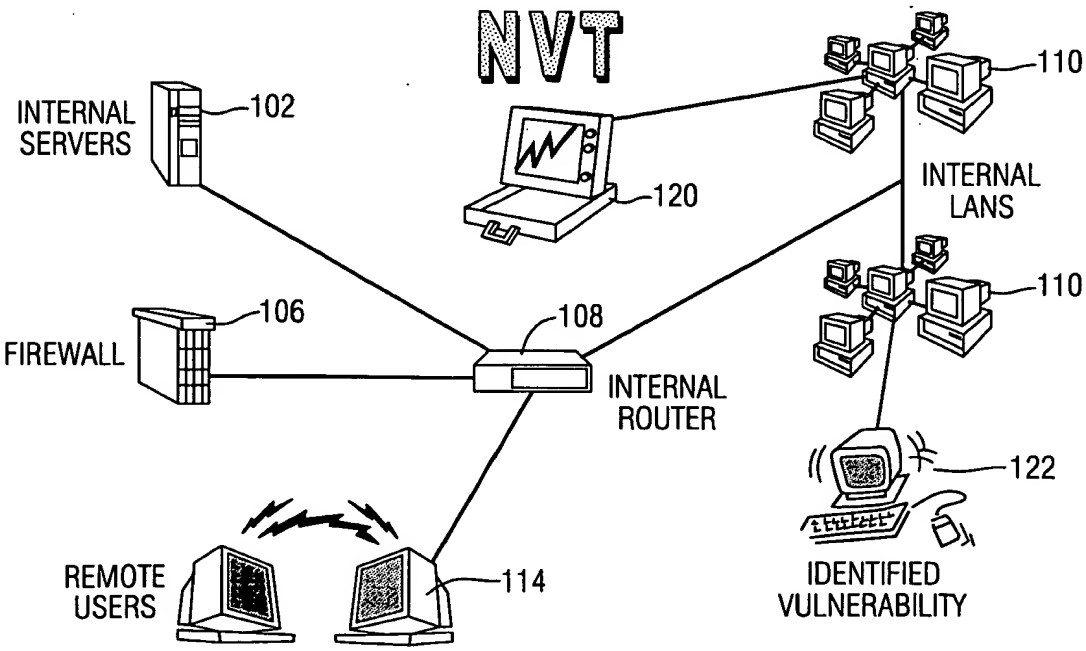

NVT
110
INTERNAL SERVERS
102
120
INTERNAL LANS
110
106
108
FIREWALL
INTERNAL ROUTER
122
REMOTE USERS
114
IDENTIFIED VULNERABILITY

FIG. 2

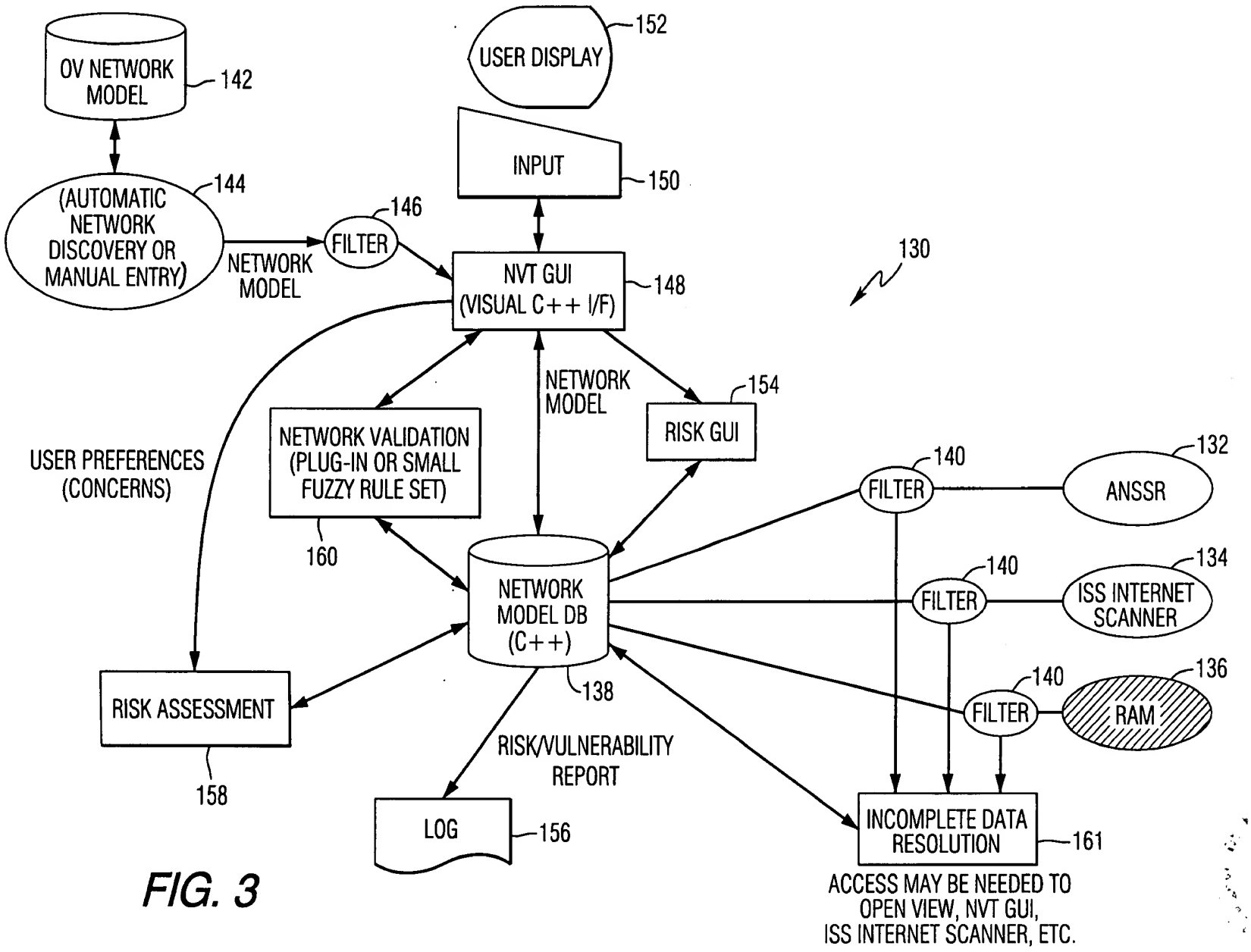

OV NETWORK MODEL
142
USER DISPLAY
152
INPUT
150
(AUTOMATIC NETWORK DISCOVERY OR MANUAL ENTRY)
144
FILTER
146
NETWORK MODEL
NVT GUI (VISUAL C++ I/F)
148
130
NETWORK MODEL
RISK GUI
154
NETWORK VALIDATION (PLUG-IN OR SMALL FUZZY RULE SET)
160
USER PREFERENCES (CONCERNS)
FILTER
140
ANSSR
132
NETWORK MODEL DB (C++)
138
FILTER
140
ISS INTERNET SCANNER
134
FILTER
140
RAM
136
RISK ASSESSMENT
158
RISK/VULNERABILITY REPORT
LOG
156
INCOMPLETE DATA RESOLUTION
161
ACCESS MAY BE NEEDED TO OPEN VIEW, NVT GUI, ISS INTERNET SCANNER, ETC.

FIG. 3

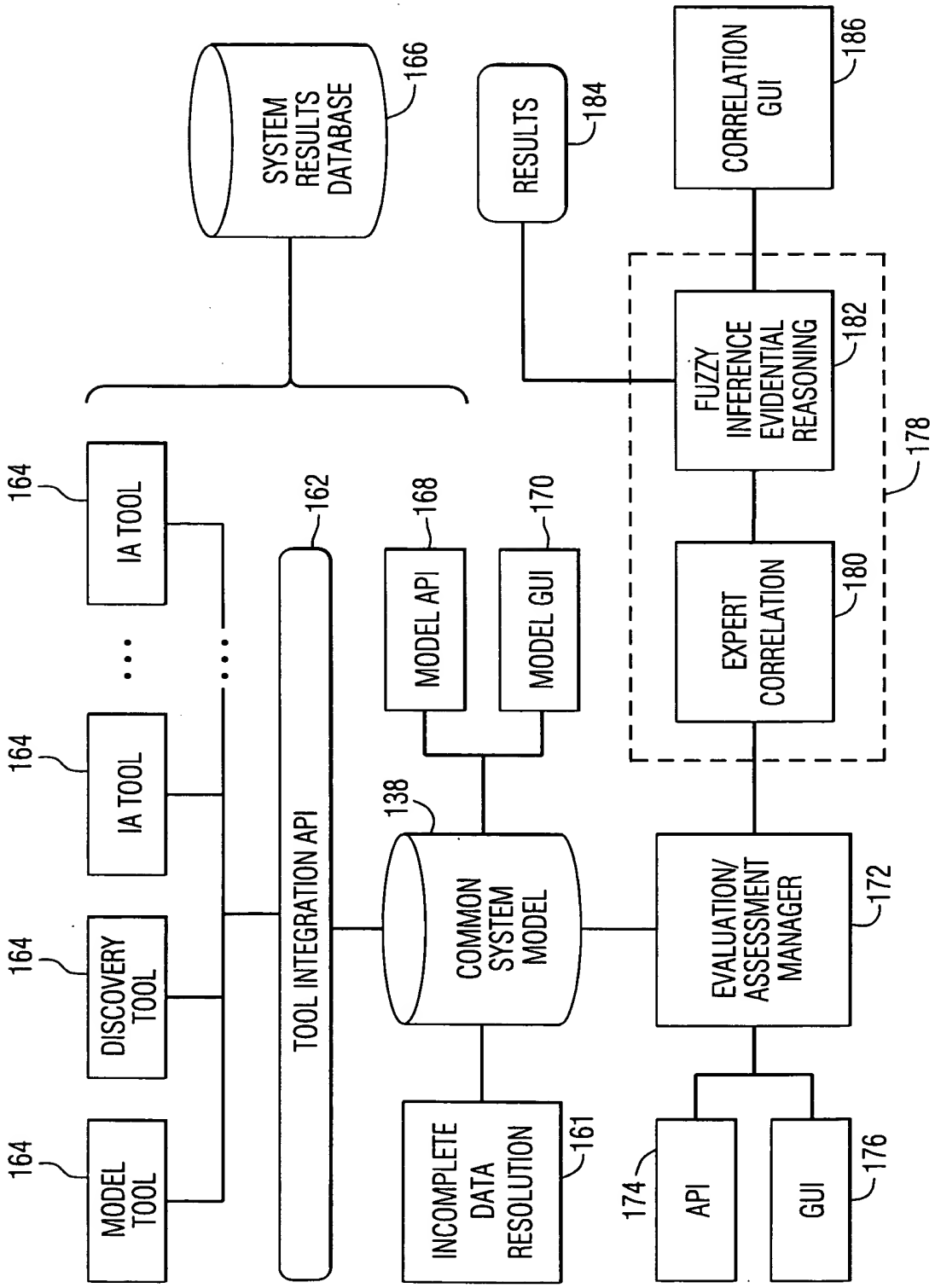

SYSTEM RESULTS DATABASE
166
RESULTS
184
CORRELATION GUI
186
FUZZY INFERENCE EVIDENTIAL REASONING
182
178
EXPERT CORRELATION
180
164
IA TOOL
164
IA TOOL
164
DISCOVERY TOOL
164
MODEL TOOL
TOOL INTEGRATION API
162
MODEL API
168
MODEL GUI
170
138
COMMON SYSTEM MODEL
INCOMPLETE DATA RESOLUTION
161
EVALUATION/ ASSESSMENT MANAGER
172
174
API
GUI
176

FIG. 4

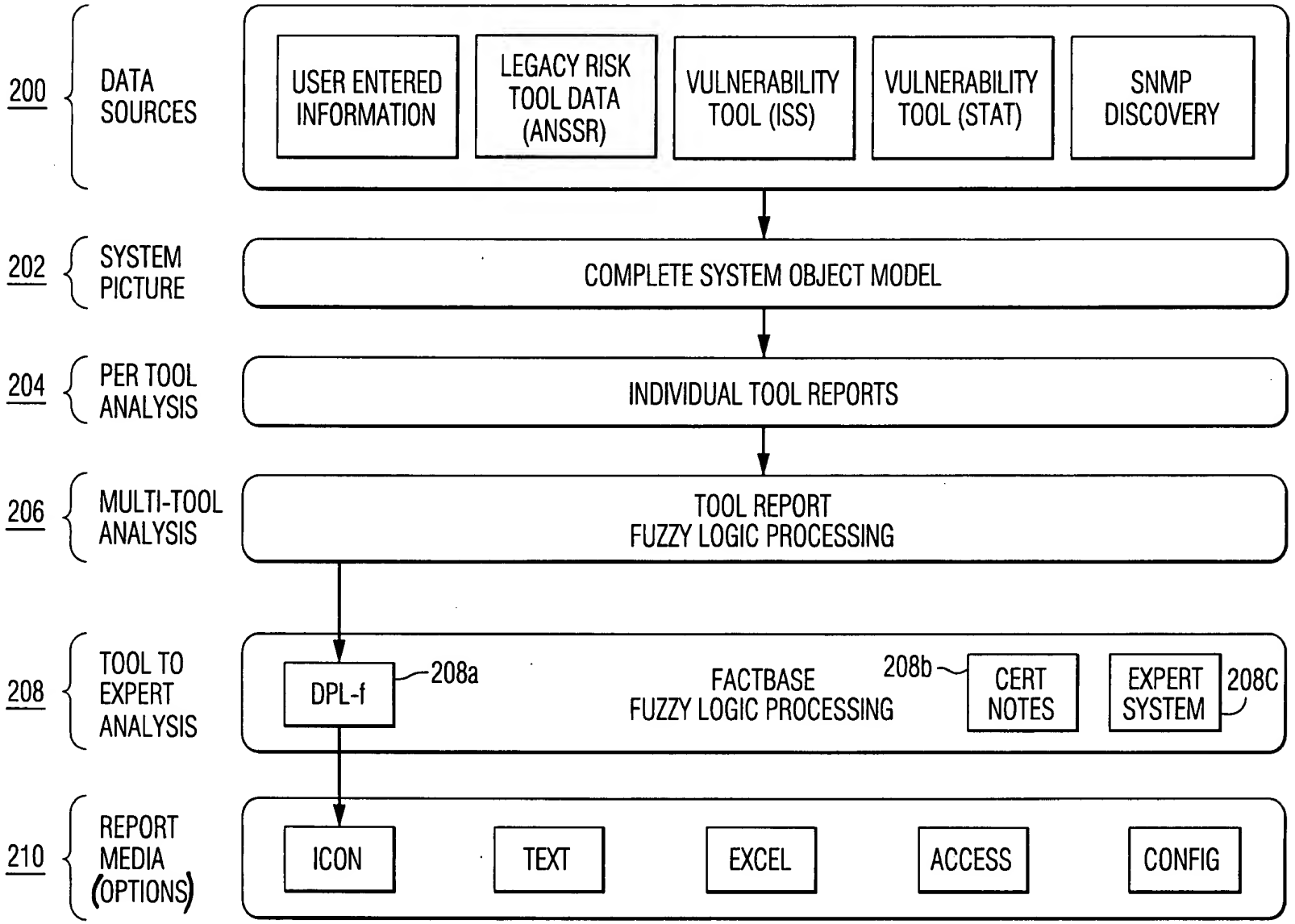

200
DATA SOURCES
USER ENTERED INFORMATION
LEGACY RISK TOOL DATA (ANSSR)
VULNERABILITY TOOL (ISS)
VULNERABILITY TOOL (STAT)
SNMP DISCOVERY
202
SYSTEM PICTURE
COMPLETE SYSTEM OBJECT MODEL
204
PER TOOL ANALYSIS
INDIVIDUAL TOOL REPORTS
206
MULTI-TOOL ANALYSIS
TOOL REPORT
FUZZY LOGIC PROCESSING
208
TOOL TO EXPERT ANALYSIS
DPL-f
208a
FACTBASE
FUZZY LOGIC PROCESSING
208b
CERT NOTES
EXPERT SYSTEM
208C
210
REPORT MEDIA (OPTIONS)
ICON
TEXT
EXCEL
ACCESS
CONFIG

FIG. 5

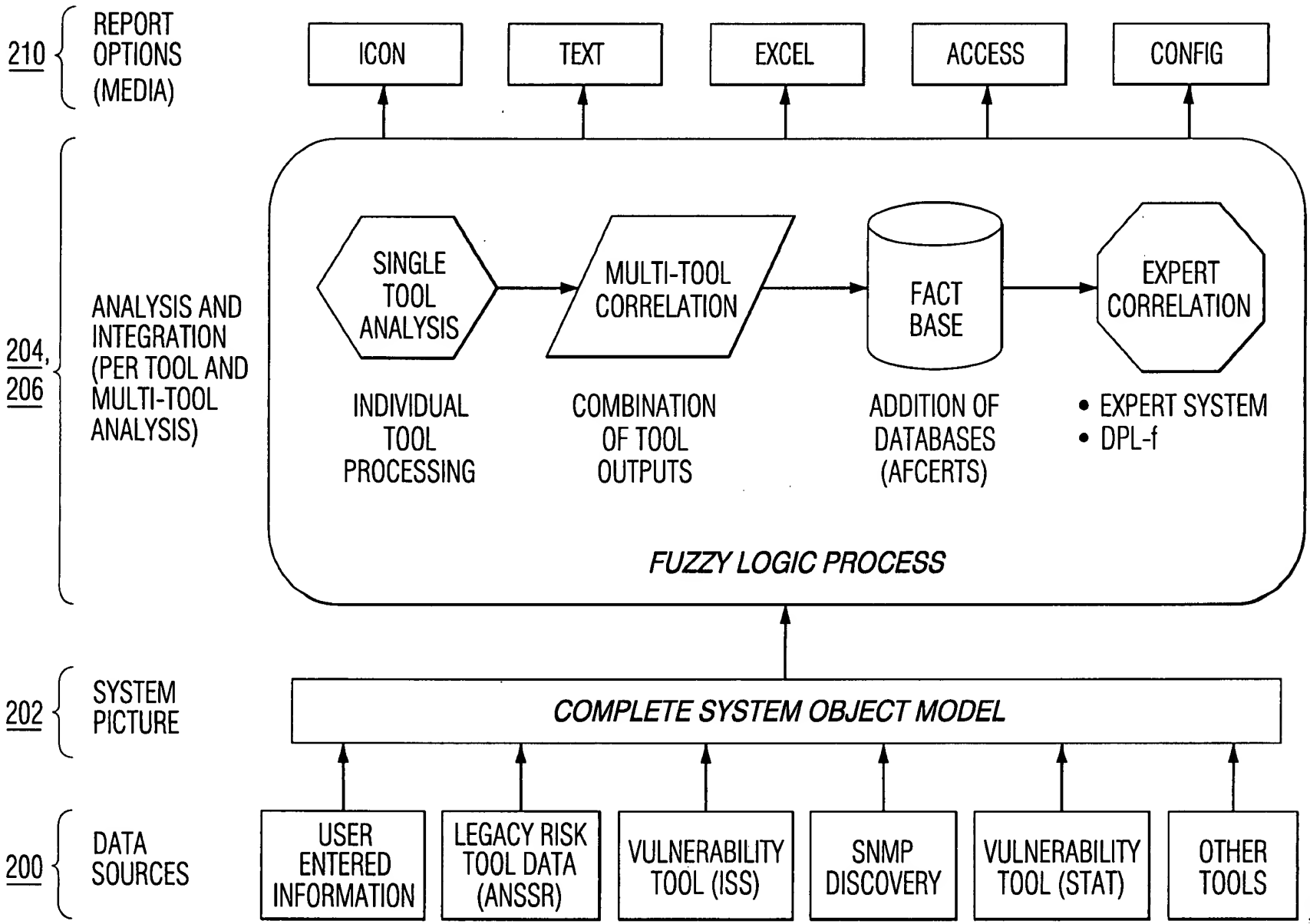

210
REPORT OPTIONS (MEDIA)
ICON
TEXT
EXCEL
ACCESS
CONFIG
204, 206
ANALYSIS AND INTEGRATION (PER TOOL AND MULTI-TOOL ANALYSIS)
SINGLE TOOL ANALYSIS
MULTI-TOOL CORRELATION
FACT BASE
EXPERT CORRELATION
INDIVIDUAL TOOL PROCESSING
COMBINATION OF TOOL OUTPUTS
ADDITION OF DATABASES (AFCERTS)
• EXPERT SYSTEM
• DPL-f
FUZZY LOGIC PROCESS
202
SYSTEM PICTURE
COMPLETE SYSTEM OBJECT MODEL
200
DATA SOURCES
USER ENTERED INFORMATION
LEGACY RISK TOOL DATA (ANSSR)
VULNERABILITY TOOL (ISS)
SNMP DISCOVERY
VULNERABILITY TOOL (STAT)
OTHER TOOLS

FIG. 6

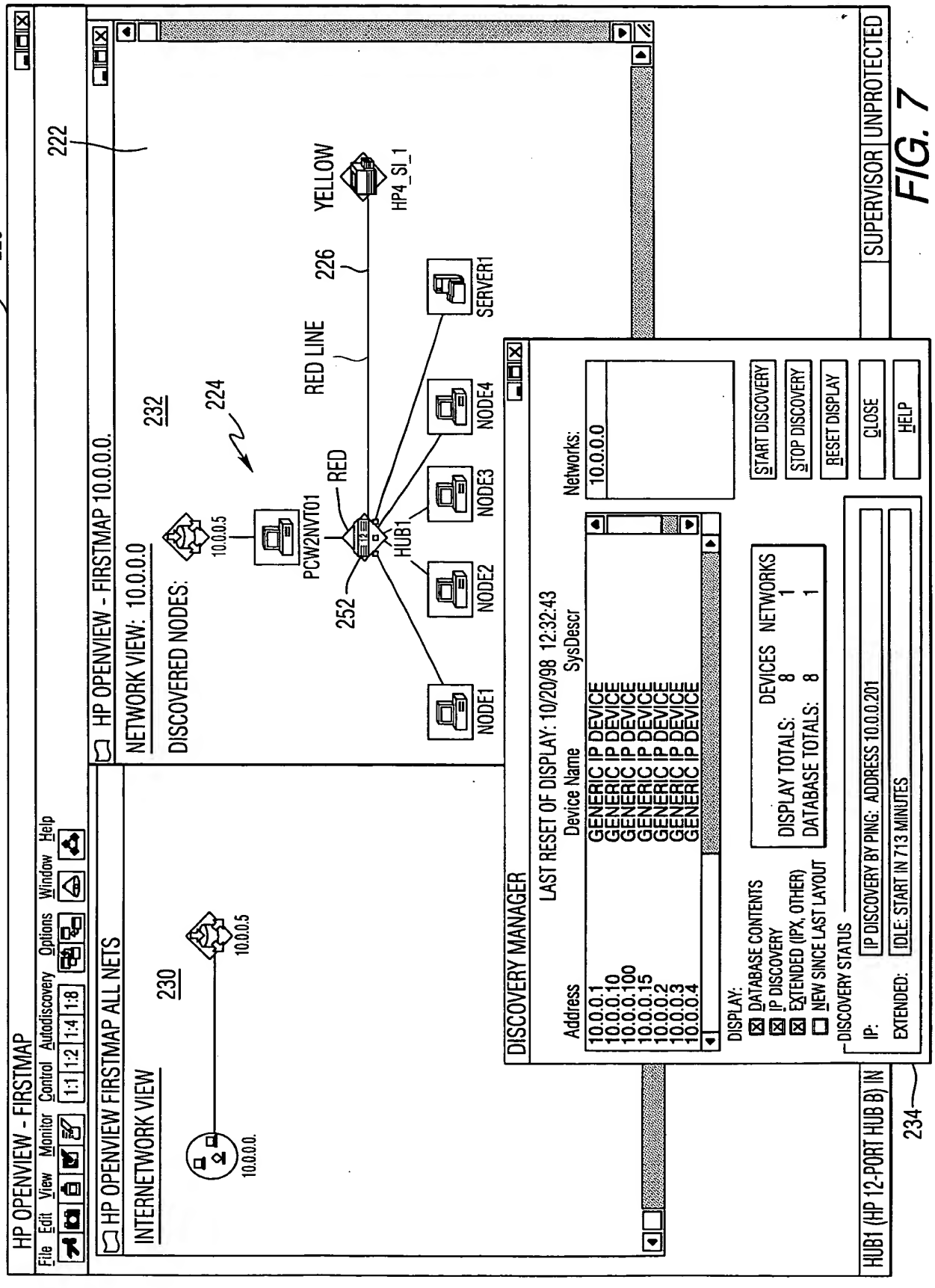

220
HP OPENVIEW - FIRSTMAP
File Edit View Monitor Control Autodiscovery Options Window Help
1:1 1:2 1:4 1:8
HP OPENVIEW FIRSTMAP ALL NETS
INTERNETWORK VIEW
230
10.0.0.5
10.0.0.0
222
HP OPENVIEW - FIRSTMAP 10.0.0.0.
NETWORK VIEW: 10.0.0.0
232
DISCOVERED NODES:
224
10.0.0.5
PCW2NVT01
RED
252
HUB1
RED LINE
226
YELLOW
HP4_SI_1
SERVER1
NODE4
NODE3
NODE2
NODE1
DISCOVERY MANAGER
LAST RESET OF DISPLAY: 10/20/98 12:32:43
Address
Device Name
SysDescr
10.0.0.1 GENERIC IP DEVICE
10.0.0.10 GENERIC IP DEVICE
10.0.0.100 GENERIC IP DEVICE
10.0.0.15 GENERIC IP DEVICE
10.0.0.2 GENERIC IP DEVICE
10.0.0.3 GENERIC IP DEVICE
10.0.0.4 GENERIC IP DEVICE
Networks:
10.0.0.0
START DISCOVERY
STOP DISCOVERY
RESET DISPLAY
CLOSE
HELP
DISPLAY:
DATABASE CONTENTS
IP DISCOVERY
EXTENDED (IPX, OTHER)
NEW SINCE LAST LAYOUT
DISPLAY TOTALS: DEVICES 8 NETWORKS 1
DATABASE TOTALS: 8 1
DISCOVERY STATUS
IP: IP DISCOVERY BY PING: ADDRESS 10.0.0.201
EXTENDED: IDLE: START IN 713 MINUTES
SUPERVISOR UNPROTECTED
HUB1 (HP 12-PORT HUB B) IN
234

FIG. 7

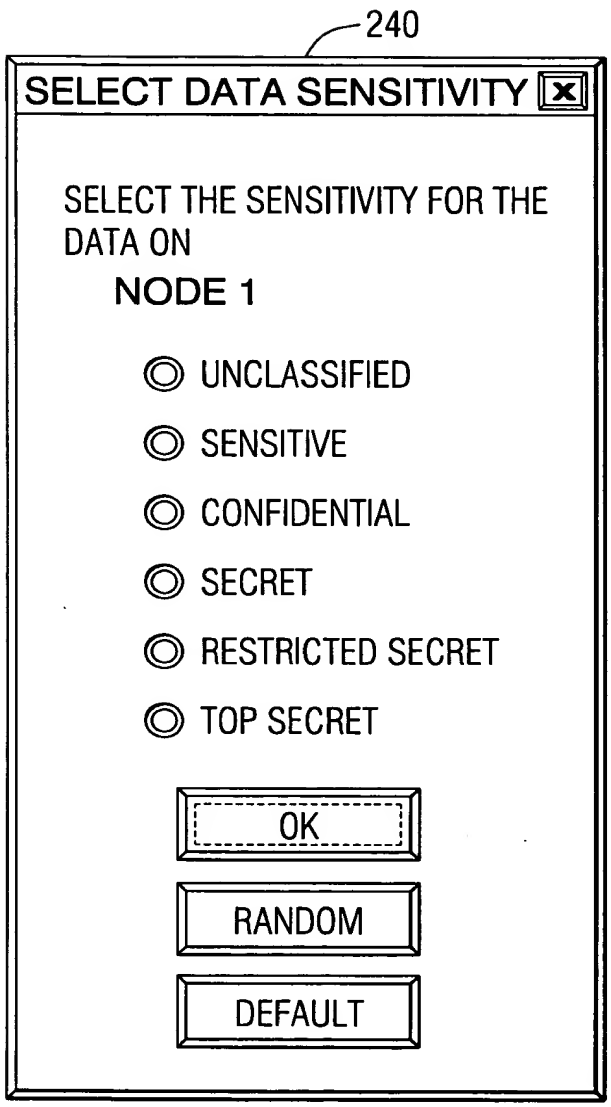

240
SELECT DATA SENSITIVITY
SELECT THE SENSITIVITY FOR THE DATA ON
NODE 1
UNCLASSIFIED
SENSITIVE
CONFIDENTIAL
SECRET
RESTRICTED SECRET
TOP SECRET
OK
RANDOM
DEFAULT

FIG. 8A

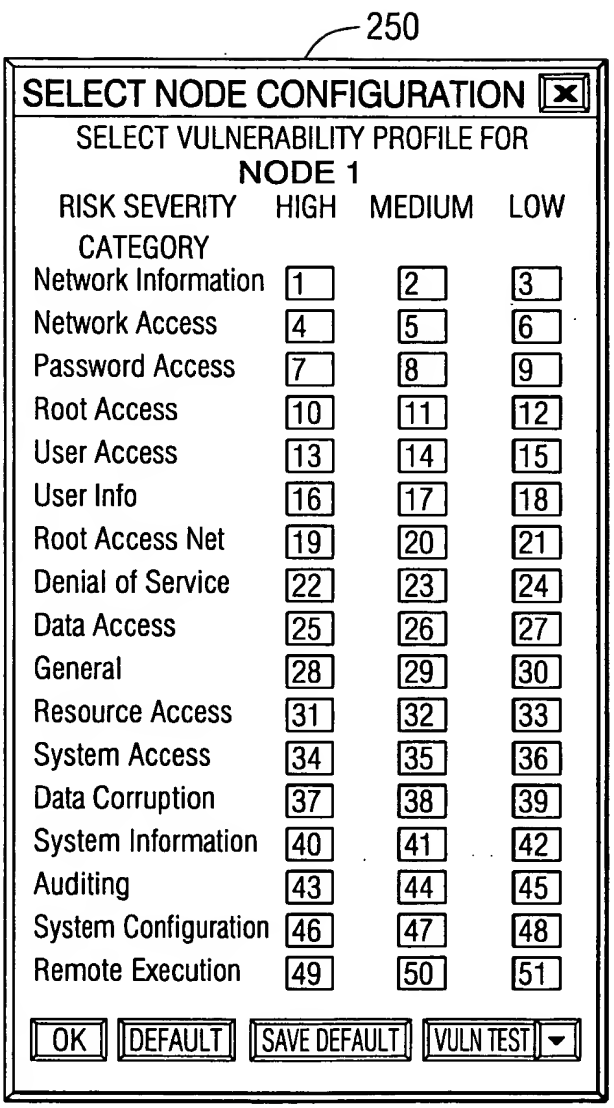

250
SELECT NODE CONFIGURATION
SELECT VULNERABILITY PROFILE FOR
NODE 1
RISK SEVERITY
CATEGORY
HIGH
MEDIUM
LOW
Network Information 1 2 3
Network Access 4 5 6
Password Access 7 8 9
Root Access 10 11 12
User Access 13 14 15
User Info 16 17 18
Root Access Net 19 20 21
Denial of Service 22 23 24
Data Access 25 26 27
General 28 29 30
Resource Access 31 32 33
System Access 34 35 36
Data Corruption 37 38 39
System Information 40 41 42
Auditing 43 44 45
System Configuration 46 47 48
Remote Execution 49 50 51
OK
DEFAULT
SAVE DEFAULT
VULN TEST

FIG. 8B

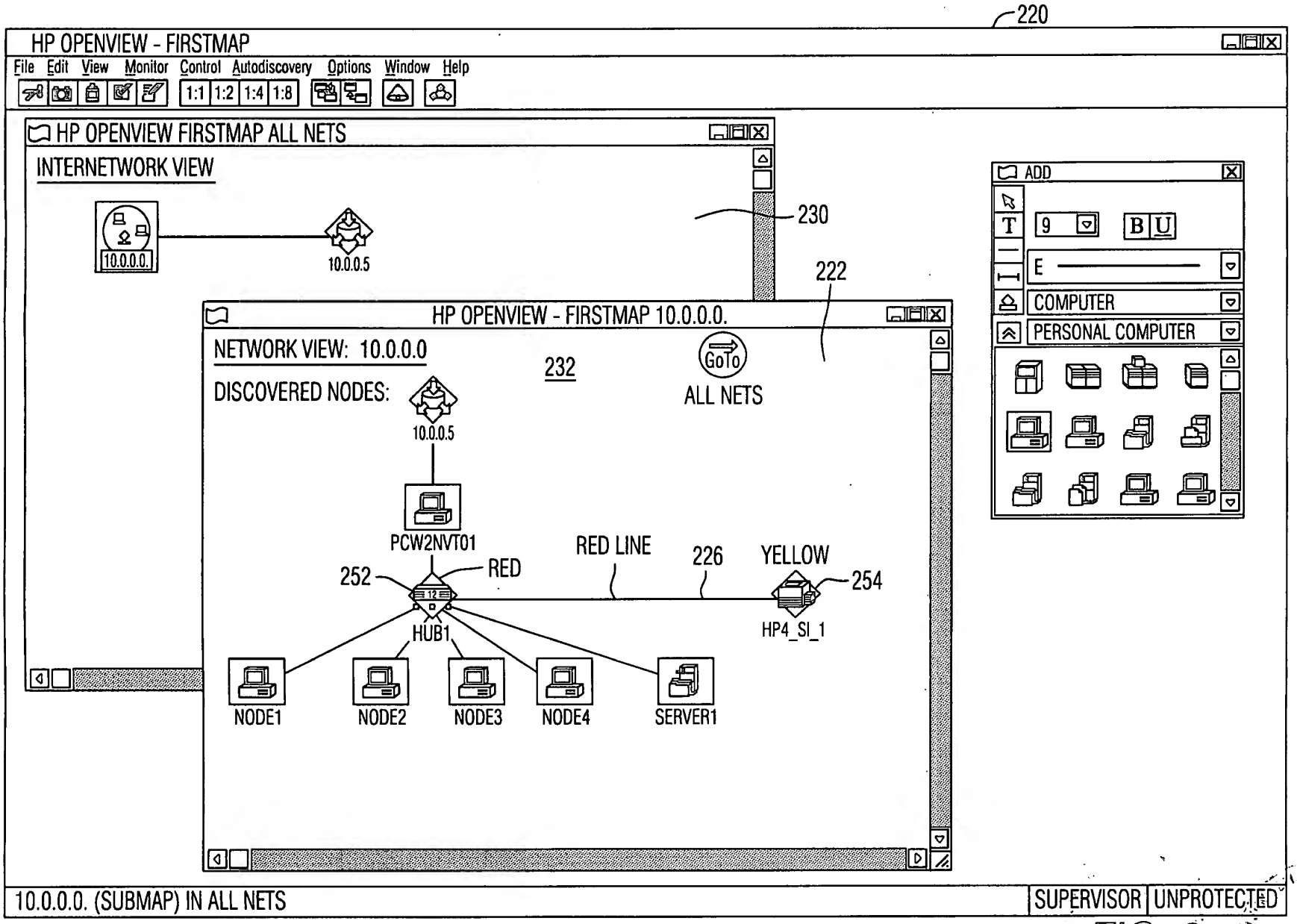

220
HP OPENVIEW - FIRSTMAP
File Edit View Monitor Control Autodiscovery Options Window Help
1:1 1:2 1:4 1:8
HP OPENVIEW FIRSTMAP ALL NETS
INTERNETWORK VIEW
10.0.0.0.
10.0.0.5
230
222
HP OPENVIEW - FIRSTMAP 10.0.0.0.
NETWORK VIEW: 10.0.0.0
232
GoTo
ALL NETS
DISCOVERED NODES:
10.0.0.5
PCW2NVT01
RED LINE
226
YELLOW
252
RED
254
HUB1
HP4_SI_1
NODE1
NODE2
NODE3
NODE4
SERVER1
ADD
9
B U
E
COMPUTER
PERSONAL COMPUTER
10.0.0.0. (SUBMAP) IN ALL NETS
SUPERVISOR
UNPROTECTED

FIG. 9

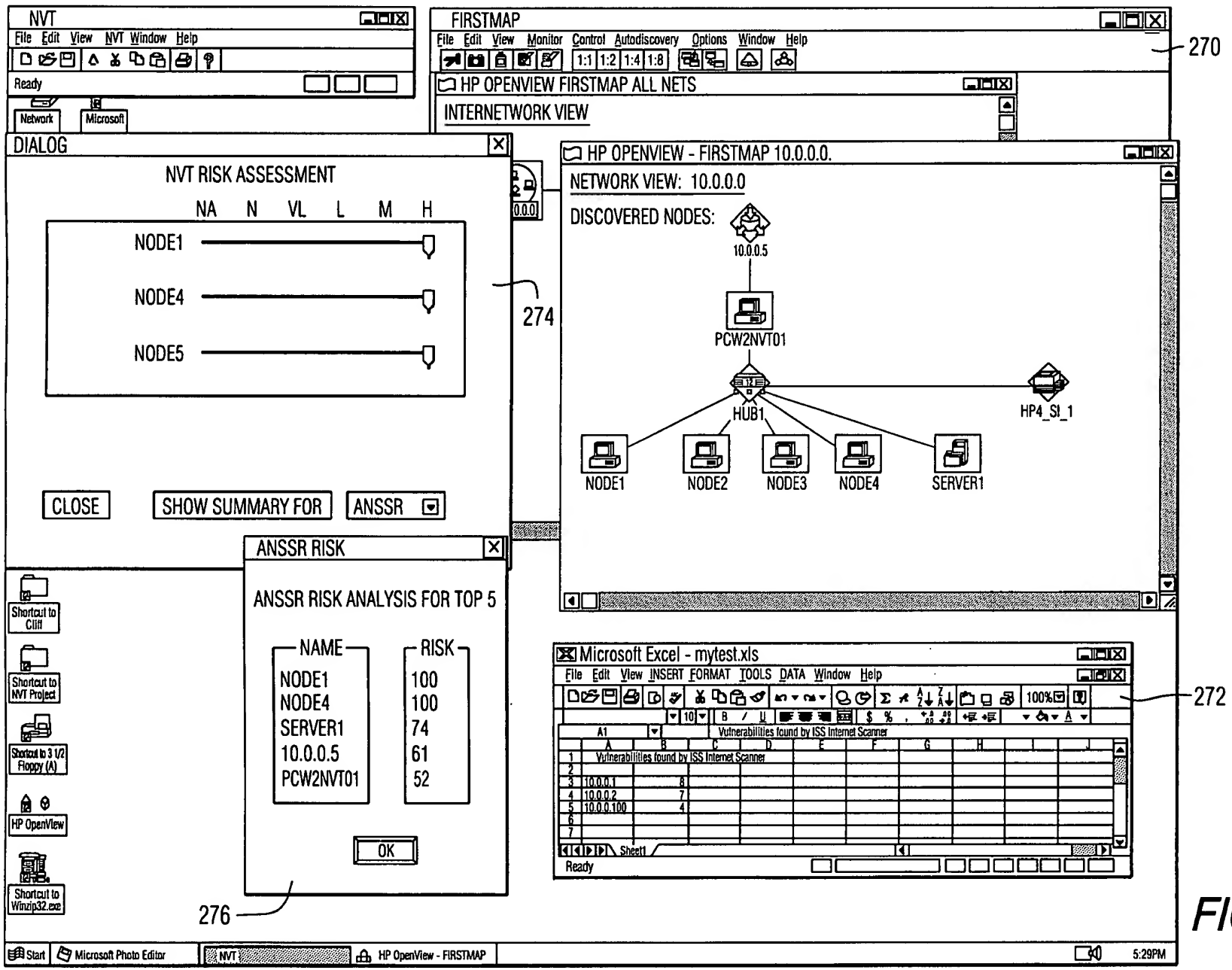

NVT
File Edit View NVT Window Help
Ready
Network
Microsoft
FIRSTMAP
File Edit View Monitor Control Autodiscovery Options Window Help
1:1 1:2 1:4 1:8
270
HP OPENVIEW FIRSTMAP ALL NETS
INTERNETWORK VIEW
DIALOG
NVT RISK ASSESSMENT
NA N VL L M H
NODE1
NODE4
NODE5
274
CLOSE
SHOW SUMMARY FOR
ANSSR
HP OPENVIEW - FIRSTMAP 10.0.0.0.
NETWORK VIEW: 10.0.0.0
DISCOVERED NODES:
10.0.0.5
PCW2NVT01
HUB1
HP4_SI_1
NODE1
NODE2
NODE3
NODE4
SERVER1
ANSSR RISK
ANSSR RISK ANALYSIS FOR TOP 5
NAME
RISK
NODE1 100
NODE4 100
SERVER1 74
10.0.0.5 61
PCW2NVT01 52
OK
276
Microsoft Excel - mytest.xls
File Edit View INSERT FORMAT TOOLS DATA Window Help
272
Vulnerabilities found by ISS Internet Scanner
10.0.0.1 8
10.0.0.2 7
10.0.0.100 4
Sheet1
Ready
Shortcut to Cliff
Shortcut to NVT Project
Shortcut to 3 1/2 Floppy (A)
HP OpenView
Shortcut to Winzip32.exe
Start
Microsoft Photo Editor
NVT
HP OpenView - FIRSTMAP
5:29PM

FIG. 10

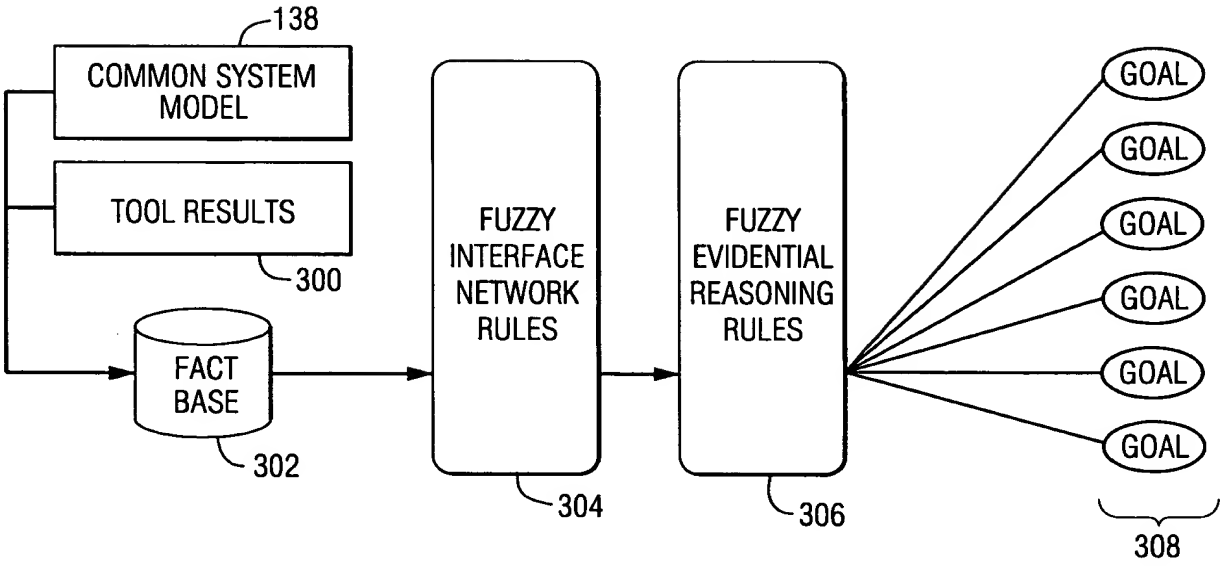

138
COMMON SYSTEM MODEL
TOOL RESULTS
300
FACT BASE
302
FUZZY INTERFACE NETWORK RULES
304
FUZZY EVIDENTIAL REASONING RULES
306
GOAL
GOAL
GOAL
GOAL
GOAL
GOAL
308

FIG. 11

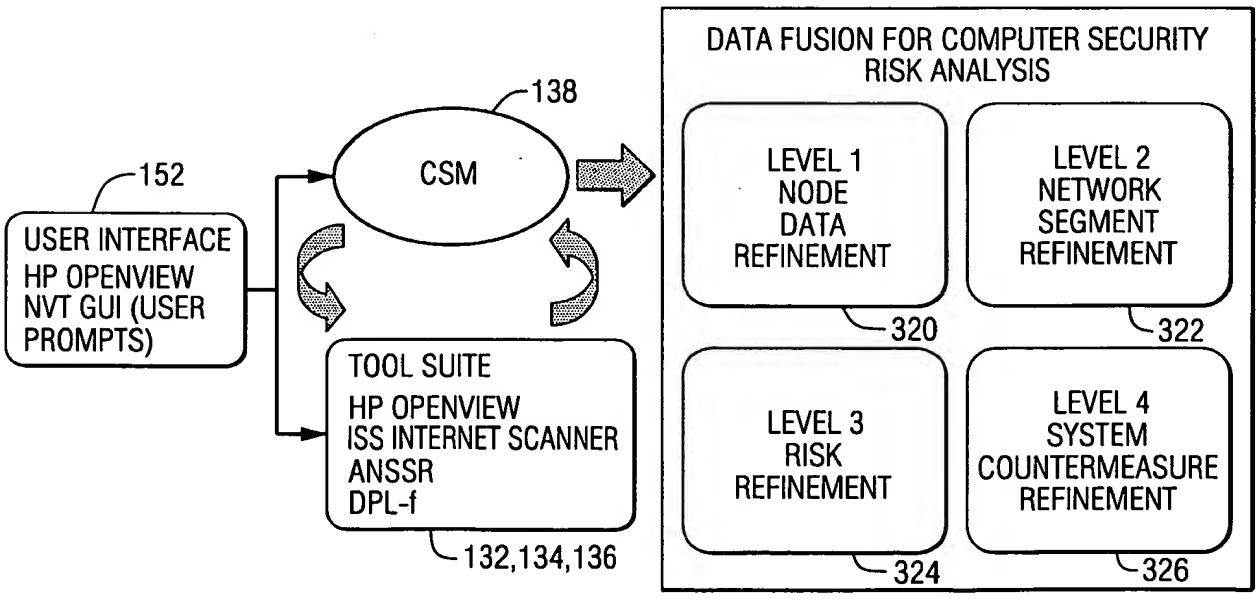

DATA FUSION FOR COMPUTER SECURITY RISK ANALYSIS
138
CSM
152
USER INTERFACE
HP OPENVIEW
NVT GUI (USER PROMPTS)
TOOL SUITE
HP OPENVIEW
ISS INTERNET SCANNER
ANSSR
DPL-f
132,134,136
LEVEL 1 NODE DATA REFINEMENT
320
LEVEL 2 NETWORK SEGMENT REFINEMENT
322
LEVEL 3 RISK REFINEMENT
324
LEVEL 4 SYSTEM COUNTERMEASURE REFINEMENT
326

FIG. 12

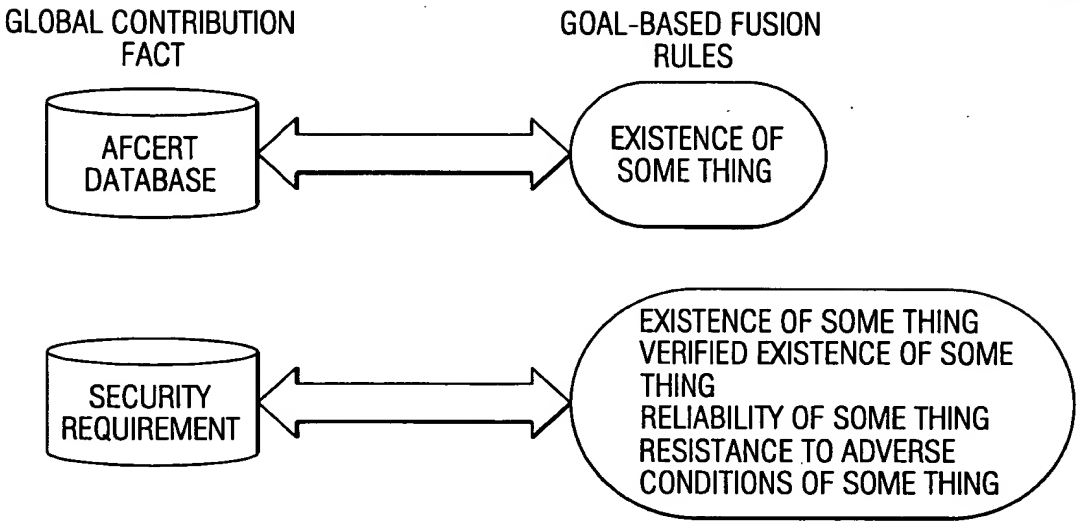

GLOBAL CONTRIBUTION FACT
GOAL-BASED FUSION RULES
AFCERT DATABASE
EXISTENCE OF SOME THING
SECURITY REQUIREMENT
EXISTENCE OF SOME THING
VERIFIED EXISTENCE OF SOME THING
RELIABILITY OF SOME THING
RESISTANCE TO ADVERSE CONDITIONS OF SOME THING

FIG. 13

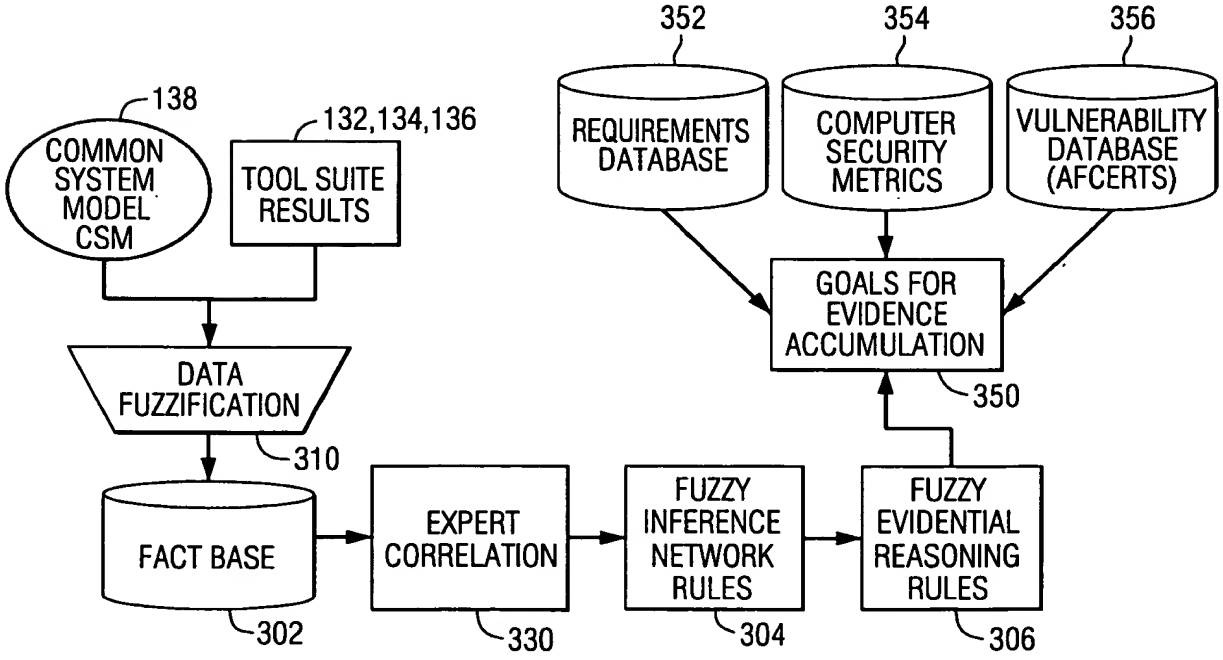

352
354
356
138
132,134,136
COMMON SYSTEM MODEL CSM
TOOL SUITE RESULTS
REQUIREMENTS DATABASE
COMPUTER SECURITY METRICS
VULNERABILITY DATABASE (AFCERTS)
GOALS FOR EVIDENCE ACCUMULATION
350
DATA FUZZIFICATION
310
FACT BASE
302
EXPERT CORRELATION
330
FUZZY INFERENCE NETWORK RULES
304
FUZZY EVIDENTIAL REASONING RULES
306

FIG. 14

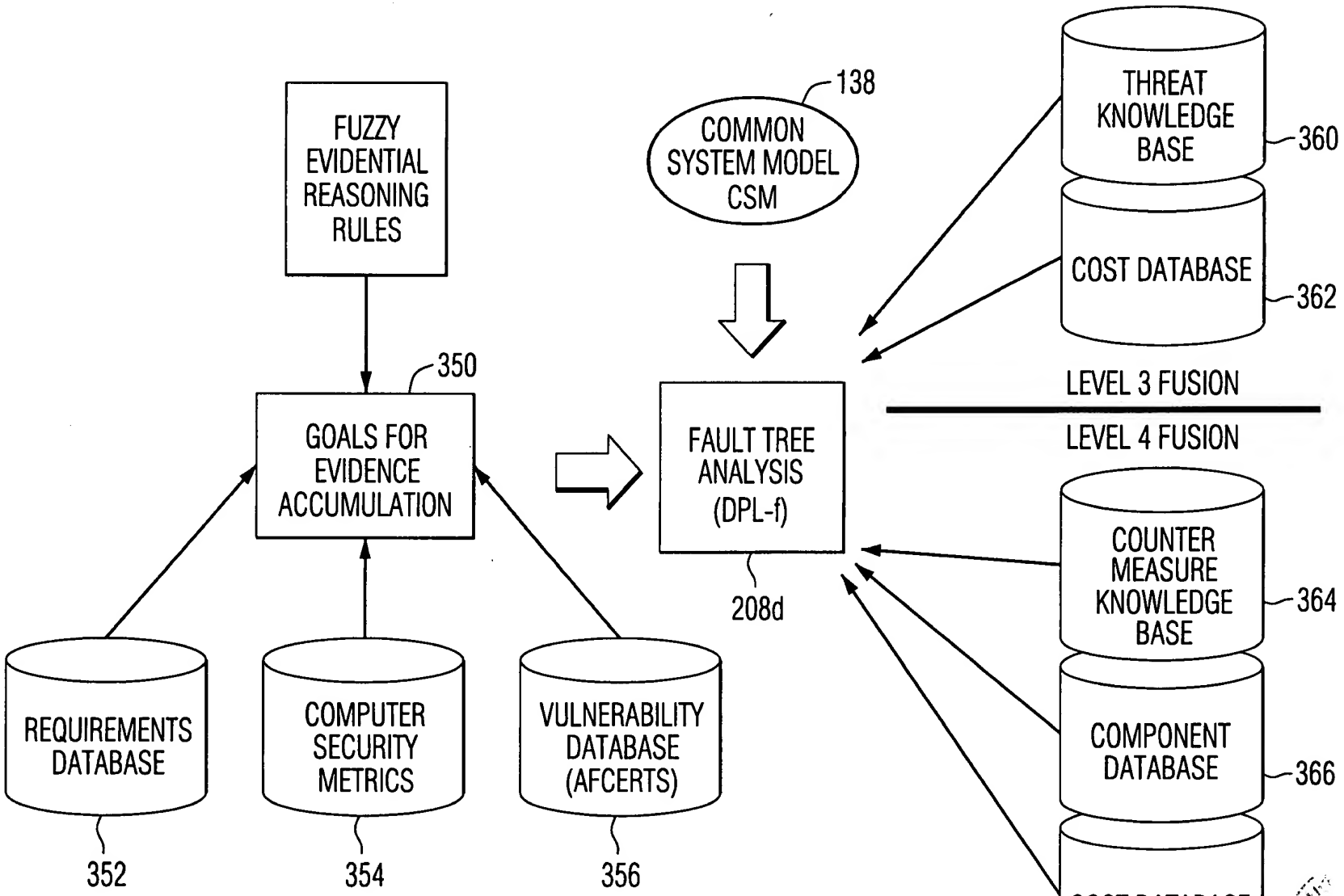

FUZZY EVIDENTIAL REASONING RULES
138
COMMON SYSTEM MODEL CSM
THREAT KNOWLEDGE BASE
360
COST DATABASE
362
350
GOALS FOR EVIDENCE ACCUMULATION
FAULT TREE ANALYSIS (DPL-f)
208d
LEVEL 3 FUSION
LEVEL 4 FUSION
COUNTER MEASURE KNOWLEDGE BASE
364
COMPONENT DATABASE
366
COST DATABASE
368
REQUIREMENTS DATABASE
352
COMPUTER SECURITY METRICS
354
VULNERABILITY DATABASE (AFCERTS)
356

FIG. 15

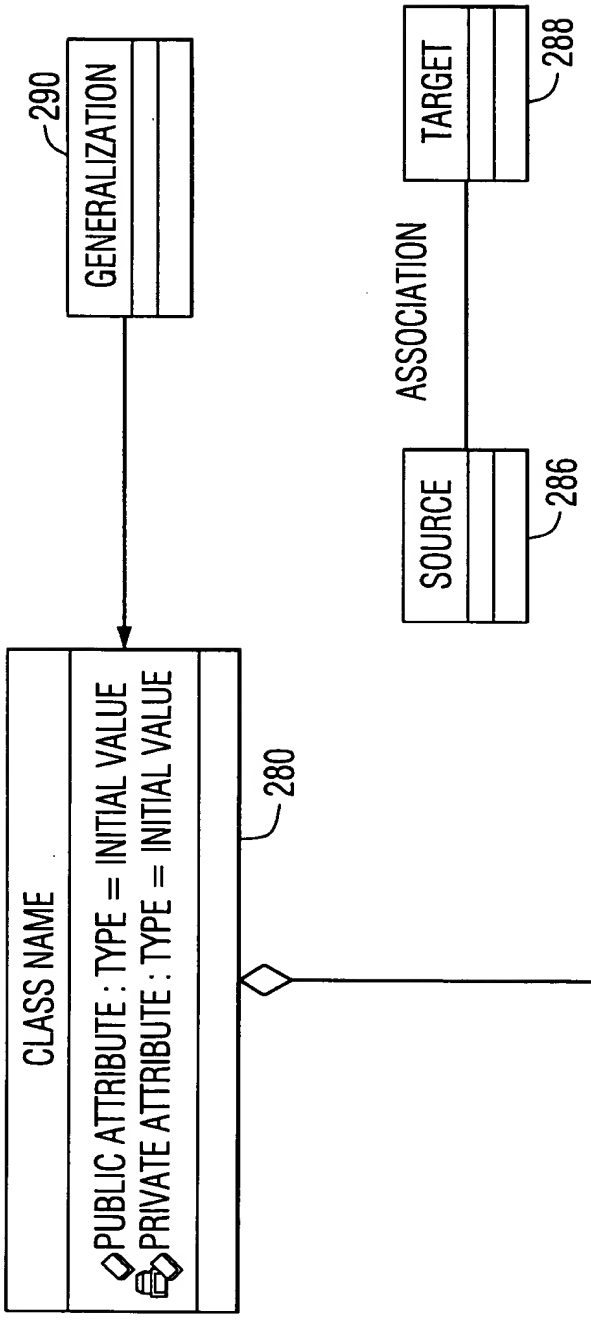
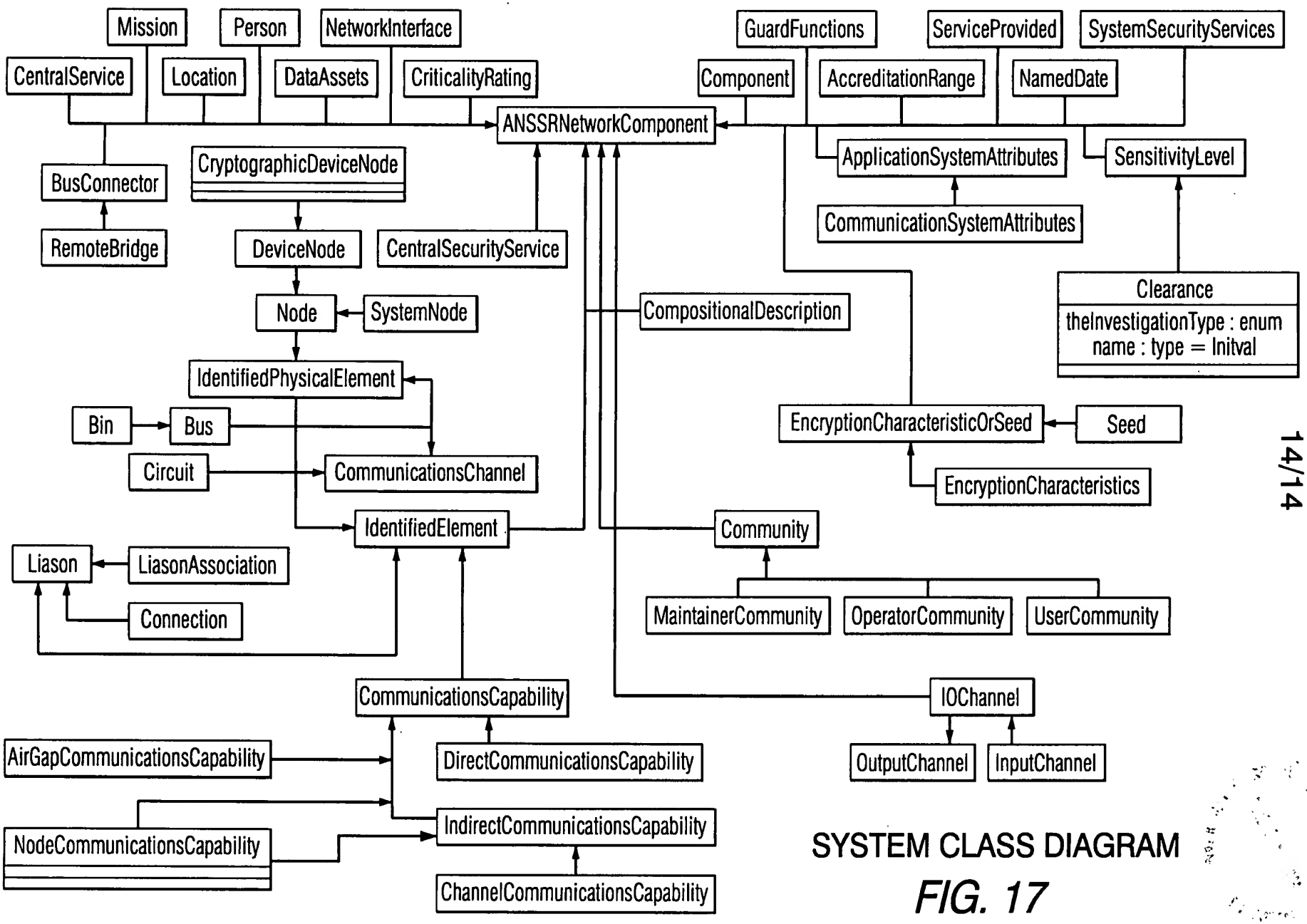

290
GENERALIZATION
TARGET
288
ASSOCIATION
SOURCE
286
CLASS NAME
PUBLIC ATTRIBUTE : TYPE = INITIAL VALUE
PRIVATE ATTRIBUTE : TYPE = INITIAL VALUE
280
AGGREGATION
284

FIG. 16



SYSTEM CLASS DIAGRAM

FIG. 17